CERT-EU: ثغرة حرجة للوصول إلى الملفات في منتجات Atlassian Data Center (CVE-2026-21589)



كشفت Atlassian عن الثغرة CVE-2026-21589 (CVSS 9.3) التي تتيح لمهاجم دون مصادقة الوصول إلى ملفات محددة في عدة منتجات Data Center. يوصي CERT-EU بالترقية بدءًا بالنسخ المكشوفة للإنترنت وفحص سجلات الوصول.

- الثغرة CVE-2026-21589 بدرجة CVSS تبلغ 9.3 وتسمح دون مصادقة بالوصول إلى ملفات محددة داخل الجذر الخاص بتطبيق الويب.
- المنتجات المتأثرة: Bitbucket وConfluence وJira Service Management وJira Software وBamboo وCrowd بإصدار Data Center، إضافة إلى Crucible وFisheye.
- يحتاج المهاجم إلى معرفة اسم الملف ومساره بدقة، ولا تتيح الثغرة سرد محتويات المجلدات.
- تفيد Atlassian بأن منتجاتها السحابية رُقّعت وأنها لم تجد دليلاً على الاستغلال.
- يوصي CERT-EU بترقية النسخ المكشوفة للإنترنت أولاً ومراجعة سجلات الوصول بحثًا عن أي

اختراق.

نشرت Atlassian في 5 أكتوبر 2026 نشرة أمنية بشأن ثغرة حرجة تتيح الوصول إلى ملفات عشوائية، وتحمل المعرّف **CVE-2026-21589** بدرجة CVSS تبلغ 9.3. وأعاد CERT-EU نشر الإرشادات ضمن النشرة 2026-015.

ما الذي تتيحه الثغرة

يستطيع مهاجم دون مصادقة الوصول إلى ملفات محددة داخل الجذر الخاص بتطبيق الويب. ويستلزم الاستغلال معرفة الاسم والمسار الدقيقين للملف المستهدف، ولا تسمح الثغرة بسرد محتويات المجلدات. وتشير Atlassian إلى أن بعض الإعدادات قد تحتوي ملفات حساسة، ما يزيد الخطر.

تشمل الإصدارات المتأثرة كل ما سبق الإصدارات المصححة في Bitbucket وConfluence وJira Service Management وJira Software وBamboo وCrowd بنسخة Data Center، إضافة إلى Crucible وFisheye. وترد الإصدارات المصححة في نشرة المورّد. وتذكر Atlassian أن منتجاتها السحابية رُقّعت وأنها لم تجد دليلاً على الاستغلال.

التعامل الموصى به

يوصي CERT-EU بالترقية إلى إصدار مصحح أو الأحدث في أقرب وقت، بدءًا بالنسخ المكشوفة للإنترنت. وتقترح Atlassian الانتقال إلى إصدار LTS المصحح أو أحدث منه.

إذا تعذّر التصحيح فورًا، تقترح النشرة إجراءات مؤقتة:

- إخراج النسخة من الإنترنت إلى حين تصحيحها، بما في ذلك النسخ التي تتطلب تسجيل دخول.
- تطبيق قاعدة حجب على جدار حماية تطبيقات الويب أو الوكيل لأنماط اجتياز المسارات، مع اختبارها بما في ذلك الصيغ المشفرة في الروابط.
- تفعيل RewriteValve في Tomcat مع ملف إعادة كتابة لمعظم المنتجات، وإضافة قاعدة حجب في ملف إعادة كتابة الروابط الخاص بـ Bitbucket ثم إعادة تشغيله، مع أخذ نسخة احتياطية أولاً.

كما يوصي CERT-EU بفحص سجلات الوصول بحثًا عن أنماط الاجتياز. وعند الاشتباه باختراق، يُحقَّق في النسخة المعنية، وتُراجع بيانات الاعتماد والأسرار المحتمل كشفها وتُدوَّر، ويُتواصل مع الجهة المختصة بالأمن السيبراني. وتتوافر مقتطفات الإعدادات الدقيقة في نشرة Atlassian.

ما يجب فعله الآن

1. حصر جميع نسخ Atlassian Data Center وCrucible وFisheye ومقارنة إصداراتها بالإصدارات المصححة في نشرة Atlassian.
2. ترقية النسخ المتأثرة إلى إصدار مصحح أو الأحدث، مع إعطاء الأولوية للنسخ المتاحة من الإنترنت.
3. إذا تعذّر التصحيح الفوري، إخراج النسخة من الإنترنت أو تطبيق قاعدة الحجب على WAF أو الوكيل أو على مستوى المنتج وفق النشرة بعد أخذ نسخة احتياطية، ثم اختبارها.
4. مراجعة سجلات الوصول بحثًا عن أنماط اجتياز المسارات، سواء بعد فك ترميز الروابط أو في السجلات

الخام.

5. عند الاشتباه باختراق، تدوير بيانات الاعتماد والأسرار المحتمل كشفها، والتحقيق في الحادثة، وإبلاغ الهيئة الوطنية للأمن السيبراني والجهة الإشرافية القطاعية بحسب الحال.